

Norton Antivirus 제거 후 Windows Defender Signature 데이터베이스가 비어 있으면 ISE Posture 실패

목차

문제

VPN을 통해 연결하는 Windows 11 25H2 엔드포인트는 ISE 상태 확인에 실패하고 규정을 준수하지 않는 것으로 표시되어 인증 및 네트워크 리소스에 대한 액세스를 방지합니다. 엔드포인트는 ISE 규칙 요구 사항을 충족하지만 VPN 연결 후 "사용자가 요구 사항을 충족하지 않음"을 보고합니다.

다음 오류가 발생하여 Windows Defender 안티바이러스 정의 버전 유효성 검사에 대한 상태 검사가 특히 실패합니다.

```
[csc_iseposture]Function: CheckOpswat::CheckOpswatProd Thread Id: 0x277C File: CheckOpswat.cpp Line: 27
```

상태 에이전트는 Windows Defender의 정의 버전 및 정의 날짜가 비어 있다고 보고하여 AUC_WIN11_IT 요구 사항이 실패하도록 합니다.

환경

- ISE(Identity Services Engine) 3.3
- Windows 11 25H2 엔드포인트
- Cisco Secure Client with ISE Posture 모듈
- ISEC 규정 준수 모듈 버전 4.3.5626.8192
- Windows Defender 버전 4.18.25080.5
- 이전에 Norton 360 안티바이러스 설치 및 제거

- ISE 포스처 시행이 활성화된 VPN 연결

해결

해결 방법에는 Norton을 제거한 다음 Windows Defender 서명을 수동으로 업데이트하고 타사 안티 바이러스와 Windows Defender 간의 공존 동작을 이해하는 것이 포함됩니다.

1단계: Windows Defender 서명 업데이트

1.- Windows 보안 설정으로 이동하여 서명 데이터베이스를 수동으로 업데이트합니다.

2.- Windows Security → Virus & Threat Protection → Windows Security → Virus & Threat Protection → Virus & Threat Protection 업데이트로 이동하여 업데이트→ 확인하십시오.

3.- 보안 인텔리전스 버전에서 비어 있지 않은 값과 현재 타임스탬프를 표시할 때까지 기다린 후 보안 상태 검증을 계속합니다.

3단계: 상태 규정 준수 확인

시그니처를 업데이트한 후 VPN에 다시 연결하고 포스처 검사가 통과했는지 확인합니다. 이제 보안 인텔리전스 버전이 비어 있지 않고 유효한 값을 표시해야 합니다.

서드파티 안티바이러스 관련 중요 고려 사항

타사 안티바이러스가 설치되어 있고 Windows 보안 센터에 올바르게 등록되면 Microsoft Windows에서는 충돌을 피하기 위해 Windows Defender를 수동 모드로 전환합니다. 패시브 모드에서는 Defender가 OPSWAT가 읽는 Windows 보안 센터/WMI API를 통해 시그니처 신선도 데이터를 게시하지 않으므로 상태 확인이 실패합니다.

이 문제를 방지하려면 Windows에서 활성 모드로 전환하는 타사 응용 프로그램을 제거하십시오. Norton 또는 기타 타사 안티바이러스 소프트웨어를 다시 설치해야 하는 경우, 이로 인해 엔드포인트

트가 다시 규정을 준수하지 않게 됩니다.

원인

근본 원인은 타사 안티바이러스(Norton)가 기본 안티바이러스 솔루션인 경우 Windows Defender 서명 데이터베이스가 부실해지기 때문입니다. Norton을 설치하는 동안 수동 모드 안티바이러스 소프트웨어에서 예약된 업데이트를 수신하지 않으므로 Windows에서 의도적으로 Defender 정의를 저장했습니다. Norton이 제거된 후 Windows Defender가 기본 안티바이러스 역할을 했지만 Windows Update 뒤에서 첫 번째 서명 가져오기가 대기되어 있고 다음 예정된 트리거에서 또는 사용자가 수동으로 강제 실행할 때만 자동으로 실행되기 때문에 서명 데이터베이스가 비어 있습니다.

OPSWAT v4 SDK 메서드 1001(GetDefinitionState)은 Defender 로컬 정의 저장소가 비어 있을 때 빈 페이로드를 반환하여 ISE Posture 에이전트가 빈 정의 버전을 ISE에 전송하도록 합니다. 그런 다음 ISE는 이 빈 값을 정책 임계값과 비교하고 엔드포인트를 규정준수를 위반한 것으로 표시합니다.

관련 콘텐츠

- [Cisco Secure Client Administrator 설명서 - 타사 소프트웨어 고려 사항](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.